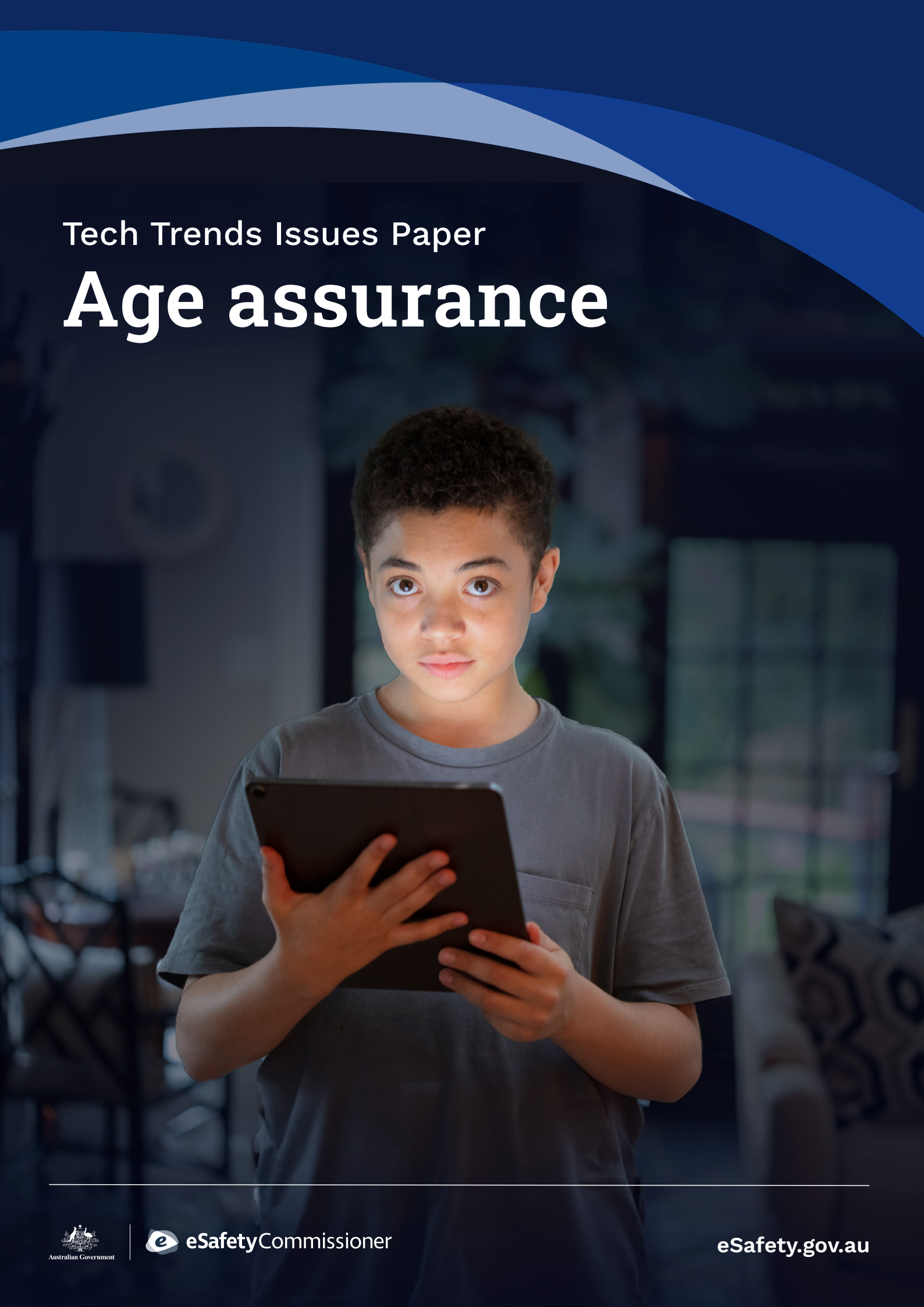
Tech Trends Issues Paper

Age assurance



Australian Government

eSafetyCommissioner

eSafety.gov.au

Contents

Background

Who we are

The eSafety Commissioner (eSafety) is Australia's independent regulator and educator for online safety under the Online Safety Act 2021 (the Act). We coordinate government efforts, conduct research, provide education, and enforce regulatory schemes to combat online harm. We work with government agencies, businesses and organisations around the world to make the internet a safer place for everyone. By staying at the forefront of online safety issues through research and dialogue with experts, we provide informed advice to the Australian Minister for Communications.

Context and eSafety's work on age assurance

In March 2023, we presented the Australian Government with a Roadmap for Age Verification (the Roadmap) which explored if and how a mandatory age verification mechanism or similar could practically be achieved in Australia. Developed through extensive stakeholder consultation and supported by novel research and a detailed Background Report, the Roadmap proposed measures to mitigate harm to children from online pornography.

You can find a reading guide to the Background Report at Attachment A.

The request to develop the Roadmap formed part of the previous government's response to the House of Representatives Standing Committee on Social Policy and Legal Affairs report, 'Protecting the age of innocence'.

As indicated in the Roadmap, eSafety will continue to monitor local and overseas developments. We will raise awareness and provide practical guidance for appropriate interventions across the digital ecosystem. This includes engaging with industry through initiatives like Safety by Design and our papers on Tech Trends and Challenges.

This paper

Our Tech Trends and Challenges program helps us understand existing and emerging online threats and opportunities. This knowledge shapes our regulatory guidance, resources, and advice to industry.

The use of age assurance is subject to debate. This paper does not delve into the merits of age assurance for specific purposes or advocate for the use of certain types of age assurance technologies. It also does not provide detailed technical assessment (see the Roadmap and upcoming trial for more information).

Rather, it provides an updated overview of different types of age assurance technology, their possibilities, limitations, risks and mitigations. It also provides a summary of current technologies and practice, and approaches to its use internationally. The paper also examines the existing policy context and evolving environment, and notes where age assurance may play a role.

While the Roadmap focuses on children's access to online pornography, this paper considers the role of age assurance in preventing a broader range of online harms to children and creating safer, age-appropriate online experiences. It references the Roadmap and Background Report and considers international and industry developments since March 2023. It also draws upon developments domestically and internationally, as well as our engagement with the online industry, since the Roadmap was released.

eSafety is committed to contributing to nuanced conversations about the proportionate and safe use of age assurance.

What is age assurance?

Age assurance refers to various methods which are used to determine a person's age. These methods offer different levels of certainty. Some determine a person's age to a very high degree of certainty (often, but not always, associated with identity verification) while others provide a range or estimation for a person's age.

Age estimation measures infer an approximate age or age range without other confirmed sources of information about the individual. This can involve the use of biometric data such as facial scans or other information such as behavioural patterns to estimate a person's age or age range.

Age verification determines a person's age to a high level of certainty, typically by verifying data against an external source. An example of age verification is using physical or digital government identity documents to verify a person's age.

Age assurance can be used online for a variety of reasons when it's important to know a user's age. This could be because the online content, environment or platform type is only appropriate for people of a certain age. For example, it ensures they're old enough to consent to their data being collected, or to access age-restricted content and experiences. Knowing a user's age is also helpful for protecting them from harmful contact, such as limiting interactions between children and unknown adults.

As noted in the United Nations General Comment No. 25 (2021) on children's rights in relation to the digital environment, the risks and opportunities for children in the digital environment vary with their age and stage of development. Therefore, state parties should respect a child's evolving capacities and consider these when designing measures to protect children or help them safely access the digital environment.[1]

How can age assurance and complementary measures counter online harm?

Determining a user's age can provide a foundation for **complementary measures** that create safe and age-appropriate online experiences. These measures can include a combination of interpersonal and educational activities, such as parents and carers supervision and having safety/wellbeing discussions, as well as technological solutions, such as age-specific or age-appropriate filters, safety settings, and parental controls. It's also important that any approach

to safety and age appropriateness offers the flexibility to adjust experiences and permissions for children as they grow and develop. Having safety measures built in and activated by default makes it easier to provide users with age-appropriate experiences. For further information, see Attachment B and eSafety's Background Report at Chapter 10.

When an online service knows the age or age range of its users, it can:

- Block access for those below the minimum age. For many social media services, this is usually 13. For services such as dating, gambling, or alcohol sales, the minimum age is 18.
- Make sure users who meet the minimum age can consent to the collection and use of their data (generally 15 under the Privacy Act) or have parental or carer consent, and enable the provision of age-appropriate materials to assist in obtaining meaningful consent.
- Offer age-specific services and experiences, such as servers, channels, groups, or functions designed for teenagers or mature audiences. Age assurance could also be used to prevent adults from pretending to be children online to access child-specific spaces.
- Apply age-appropriate safety settings, such as making accounts private; limiting access to certain communication tools, purchases, or downloads; or limiting interactions with other users.
- Adjust content filtering, moderation, and/or recommender algorithms to prevent or limit younger users seeing inappropriate content, advertisements, or accounts. This can help reduce unintentional and unwanted encounters and may assist in reducing unhealthy content bingeing or rabbit holes.

However, if users provide false birth dates when accessing a site or setting up an account, and services only rely on this information, these safety measures may not be enabled or effective. For example, if an 8-year-old pretends to be 13 when signing up for an account, by the time they turn 13 their account might appear to be 18+ and teen-specific safety measures won't apply. Research commissioned by Ofcom in 2022 found a third of children aged 8 to 17 had adult social media accounts.[2]

In December 2023, Ofcom published a report on how video-sharing platforms (VSPs) are protecting children from encountering harmful videos.

The report, focused on TikTok, Twitch and Snap services in the UK, found the services rely on users declaring their correct age during sign up. They also use a range of methods including AI and human moderators to detect potential underage accounts, but the report noted the effectiveness of these methods is yet to be established.

Services should assess the risks to children and put in place compliant, proactive, and proportionate measures to address those risks. While user safety is a shared responsibility, the burden of safety should never fall solely on the user.

A Safety by Design approach makes sure services are proactive in creating safe, age-appropriate experiences. This minimises online harm from the start and throughout their use and lifecycle. It includes thinking about the roles and responsibilities of other services in the digital ecosystem and working together where possible. This ensures the right measures are being introduced at different stages of a user's online journey. For example, websites offering services or content that's not appropriate for children can apply 'restricted to adults' meta-tags, which signals they should be filtered or blocked at an ISP, device, or search level if relevant safety settings have been enabled.

In chapter 5 of the Background Report, eSafety examined the evidence concerning the impacts and potential risks to children from accessing age-inappropriate material, specifically online pornography. Chapter 8 of the Roadmap further explored emerging evidence and the expanded scope for harm as new technologies, such as generative AI and immersive technologies, converge. We discuss the potential for age assurance and other important complementary safety measures for these technologies through our series of tech trends papers available on our website.

These approaches are not mutually exclusive and multiple measures can work together to apply age restrictions to online goods and services. For example, a social media service might use age gates based on users' self-declared age while also using AI profiling and user reporting mechanisms to detect potential underage accounts.[3]

Public sentiment about these approaches varies and there is generally low awareness among the public about many of these methods.[4]

Snapshot of current practice

Several services are trialling or implementing age assurance technologies for parts of their service in Australia.

Social media, gaming and online video streaming*

Google – YouTube users in Australia can confirm their age by providing credit card details or a copy of a valid government ID.[5] This allows them to view age-restricted content. Google also uses machine learning to identify users who may be underage, and then requires those users to provide verification using the above methods. Classifiers are also used to identify 'young minors' who are livestreaming on YouTube. These accounts are then assessed by a human moderator.[6]

Yubo reports that it has verified the age of all its users worldwide, including Australian users.[7] This is done through facial age estimation or user ID. Yubo uses this information to group users into communities around the same age.

Meta – For **Instagram,** users must declare their date of birth when setting up an account. If Australian users later try to change their age from under 18 to over 18, Meta requires them to confirm their age. They can do this by submitting a government ID or by taking a video selfie using facial age estimation technology.[8]

TikTok users must declare their date of birth when setting up an account. TikTok uses proactive detection (automated and human moderation) to detect underage users, including through language analysis and user reporting. If an account is mistakenly flagged as underage and shut down, users can appeal and demonstrate they are over 13 using facial age estimation technology, credit cards or a selfie with a government ID.[9]

Tinder is trialling ID and photo verification (video selfie and a valid driver's licence or passport) to protect users from scams. Verified users can display a check mark on their profiles. However, verification is not necessary to create an account.[10]

Roblox has partnered with Persona, an online identity verification company, to verify the age of users. This allows users to access content and experiences suitable for ages 17 and up. Verification is done using a government ID and real-time matching to photo identification.[11]

Snap registration requires a date of birth and registration fails if a user is under the age of 13 years, according to Snap's response to a transparency notice from eSafety in 2022.[12] It said that if Snap is made aware that a Snapchat user is under the age of 13 years by another user, a parent or law enforcement report, Snap terminates the

* These services may likely fall under Social Media Services, Designated Internet Services and Relevant Electronic Services for the purposes of the Online Safety Act and the Industry Codes and Standards.

account and deletes the user's data. Snap also stated it prevents users who have previously indicated they are 13 to 17 years old from updating their year of birth to an age over 18 years.

Twitch uses a range of measures to ascertain users' ages, including self-declaration upon sign-up, analysis of text entered by users, traffic analysis and parental report submissions.[13]

Alcohol

NSW has piloted the use of its Service NSW app as proof-of-age for alcohol purchases. This allows users to confirm they are 18 or over without providing extra information to alcohol retailers.[14]

Gambling

Online gambling platforms in Australia must verify users are 18 or over when they create an account and before they can place a bet. This became a requirement in September 2023.[15] For example, Sportsbet allows users to verify themselves by submitting a driver's licence, passport, Medicare card, or superannuation or payroll information.[16]

Age assurance technology is being used by services internationally. Examples include Facebook Dating in the US,[17] and on PlayStation accounts in the UK and Ireland.[18]

Many of these services are using age assurance for limited jurisdiction or limited services. While expansion or continuation of use suggests these platforms are finding the measures successful, to date there is limited independent or regulatory assessment.

OnlyFans in the UK now requires fan accounts to verify they are over 18. Since August 2021, users can use Yoti's facial age estimation.[19] Previously, only creator accounts (those that create and post content) needed to do these age verification checks. In Australia, fan accounts must provide a credit card as a form of verification to access content.

On 1 May 2024, Ofcom opened an investigation into OnlyFans. As a video sharing platform, OnlyFans must implement appropriate measures to protect children under the age of 18 years from encountering age-restricted material. OnlyFans is also obligated to provide complete and accurate responses to statutory information requests.

On 6 June 2022 and 23 June 2023 Ofcom sent OnlyFans two notices seeking information to understand and monitor OnlyFans' measures to protect children from encountering restricted material and to enable Ofcom to publish a report regarding how OnlyFans and other video

sharing platforms are protecting children from restricted material. Ofcom is investigating whether OnlyFans have breached their statutory requirements. Ofcom expect to be able to provide an update on the investigation in August 2024.[20]

How and when age assurance can be applied

Age assurance can be implemented at various stages of a user's online journey, depending on the risks associated with the service or content.

Age assurance measures could be applied at the following points:

- **Accessing a specific site, app or service.** For example, asking users to declare or prove their age at a landing page before they can view the remainder of a site. Checks can also be used to confirm a person is below a certain age.
- **Proactive detection.** Some services employ technology or human moderators to detect and remove underage users from their platforms. This can be done through tools using behavioural signals or language analysis.
- **Account sign up**. Many services ask users to declare their age and/or date of birth when creating an account.
- **Accessing specific features or content on a service.** In some cases, users only need to provide or verify their age if they want to use features not suitable for children or that pose a higher risk of harm. In Australia, services with R18+ material must implement an access-control to the content.[21]
- **Adjusting a previously entered age**. For example, to confirm the age of users who try to edit their date of birth from under 18 to 18 or over.
- **Responding to a flag or report.** If a user's actions suggest their declared age is false, platforms could require them to verify their age. This could be in response to reports from other users or from AI behavioural scanning.

Everyone in the digital ecosystem has a role in creating safer online environments and should consider when age assurance can be implemented in their services or products. For example, age assurance can also be applied at other key points:

- **Connecting to the internet**. UK mobile network operators block 18+ content on their services unless a user proves they are an adult. They can do this online or over the phone with a credit card, or in store with a photo ID. Ofcom's draft guidance supporting

the implementation of the UK's Online Safety Act,[†] suggests this check could be shared with other services as a valid age check.[22] In Australia, ISPs keep details of the account holder, who is typically over 18. They offer parental controls and filtering options, but these are not default settings and are not linked to age checks.

- **Device level**. Native apps on device operating systems, such as Apple's Screen Time, Google's Family Link and Microsoft's Family Safety, offer parental control and filtering options. This infrastructure could be used for age checks to ensure features, apps, sites and services used on devices are age appropriate.

These age check points could also rely on age attributes (e.g. '18+') shared by the user across an ecosystem. See discussion below on zero-knowledge proofs and eSafety's Background Report for more about sharing age information. Pre-existing internet ecosystems could be a potential way to leverage pre-existing information gathering processes for privacy-protecting, data-minimising age assurance and complementary safety measures.

Ecosystems of online services can exist where products including online services are interconnected, for example through integration, pre-installation and common user accounts.[23]

eSafety supports a response that involves all services, products, and platforms, such as devices' operating systems, app stores, and search engines, in reducing access to content that may not be age appropriate.

Challenges and mitigations

eSafety's Background Report evaluates various age assessment methods, highlighting their advantages and disadvantages. These vary based on the method, its implementation, and the context of use.

This section talks about concerns with different technologies and suggests ways to mitigate specific risks. The criteria eSafety devised to evaluate technologies for the Roadmap are included at Attachment C.

For a detailed assessment of different age assurance methods, including data sensitivities, privacy, accessibility, bias and effectiveness as of March 2023, see chapter 8 of eSafety's Background Report.

[†] Ofcom's draft guidance outlines examples of age assurance methods which could be considered 'highly effective' for the purposes of the UK's Online Safety Act. Their examples include mobile-network operator (MNO) age checks. In the UK, MNOs automatically apply a content restriction filter which prevents children from accessing age-restricted sites. Users can remove the filter by proving that they are an adult. The removal of the filter indicates that the user of the device is over 18 and this information can be shared with relying parties. For more information on Ofcom's draft guidance, see Attachment C.

To supplement the Roadmap, eSafety commissioned an independent review of various age assurance and safety technologies, as well as relevant international standards. We published this report with the Roadmap. As technology advances and new assessments and tests emerge, we will continue to update our information and understanding of the current market.

Privacy, security, and data collection

Privacy is crucial for everyone's agency, dignity, and safety. Age assurance technologies can pose privacy risks due to the type and amount of data they collect, store, use, and share. Products that verify age using identity documents may collect personal information such as names, birthdates, and addresses. Age estimation products may access biometric information such as facial images or videos.

Age assurance and parental control tools must proactively address privacy concerns related to users' data, including identity, activities, location, communication, emotions, health and relationships. Collected data must be handled in a privacy-conscious manner.

The following strategies may reduce privacy risks:

- **Implement enforceable standards:** Enforce standards and independent accreditation and oversight of age verification systems and providers. This could include mechanisms for complaints and redress for data or privacy breaches, restrictions on data collection, use and sharing of data, requirements for data deletion or maximum retention periods, and restrictions on profiling and tracking.
- **Design systems and processes to minimise data use:** Collect data only for its intended purpose and give users clear, accessible and meaningful information about how their data is collected, used and stored. While IDs are often used to verify age, **it is not necessary to identify users to determine their age**.
- **On-device age analysis:** Perform age analysis on the user's device and delete the input once the analysis is complete to avoid retaining data.
- **Use re-usable verifications or 'tokens':** This may help to reduce user friction and minimise the frequency of personal information sharing. Instead of revealing a user's specific age, these tokens can be limited to confirming whether a user meets a minimum age requirement. Age tokens can be stored on a user's device in an app, digital wallet or through cookies.
- **Apply a double-blind or zero-knowledge proof method:** This is to share an estimated or verified age, where information can be provided to a verifying party without revealing further details. This could involve a third-party exchange that transfers information (with a person's consent) between services requiring age confirmation and age assurance tools. The exchange only transfers information the user agrees to disclose, allowing age verification without

sharing other identifiable data. Zero-knowledge proof methods are currently in development and are not yet commercially available.

Biometrics and privacy

In January 2024, the UK Information Commissioner's Office (ICO) updated its opinion on age assurance for the Age-Appropriate Design Code (also known as the Children's Code).[24] This update, which replaces the 2021 opinion, considers the obligations of providers under the UK Online Safety Act and the technological advancements since 2021. It highlights the increased use of facial age estimation technology. We refer to the 2021 opinion throughout our Background Report. The updated advice outlines the main data protection principles and requirements that services in scope of the Children's Code must consider in the context of age assurance. It provides specific guidance on age estimation, AI and biometric data, whether it's used for recognition (matching a live face to a photo ID) or classification (estimating age from a face).

Biometric data is considered special category data under the UK General Data Protection Regulation (GDPR) when used for identification but may not be classified as such when used for estimation/assessment as it does not 'identify' a user.

Under the current Australian Privacy Act, biometric information is considered sensitive information. The Australian Government response to the Privacy Act review supported the proposal that the Office of the Australian Information Commissioner (OAIC) should continue to develop practice-specific guidance for new technologies and emerging privacy risk. The government also agreed there should be further consideration of enhanced risk assessment requirements for facial recognition and other uses of biometric information.

In **France**, the Laboratoire d'Innovation Numérique de la CNIL (Digital Innovation Laboratory of the CNIL LINC) conducts experimental projects and develops prototype tools, services and concepts related to data. In June 2022, LINC released an open-source demonstration of the zero-knowledge proof method. This method lets individuals prove their age without having to reveal any other information to services that restrict access based on age. In July 2023, LINC released a follow up piece, proposing how these methods can be monetisable, without undermining the double-anonymity system.[25]

Meanwhile, **Spain** has plans to develop similar technology. Users will be able to share their age to access age-restricted websites using an app, QR code or digital certificate. This technology is expected to be available mid-2024.[26]

euCONSENT is exploring how to monetise zero-knowledge proof methods of age assurance by proposing the use of a 'tallying service'.[27]

euCONSENT aims to develop a device-based age assurance app that stores anonymised age assurance tokens. Users would choose an age assurance provider within the euCONSENT network. After verifying the user's age, the provider would issue a token, stored in the app, which would only reveal cryptographically signed information of the user's age qualification and no other identifying information. When visiting age restricted sites, users can present their age verification token. The use of the specific age assurance provider would be added to a total count maintained by the euCONSENT tallying service to allow invoicing. This tallying service would know only the number of tokens used by each website and the age assurance provider that issued each token, maintaining user privacy and the zero-knowledge proof nature of the age assurance system.

euCONSENT's device-based approach also aims to integrate with the European Union (EU) Digital Identity Wallet. For more information about the EU's digital identity initiatives see Attachment D.

Currently, this system is still in development and has not been implemented by euCONSENT.

Accuracy and level of assurance

Age assurance methods vary in their accuracy and robustness. Making direct comparisons of accuracy is challenging because of the variety of approaches they use. Methods that verify ages against government documents are often highly accurate, but they are still subject to fraud or spoofing.[‡] Methods that estimate age can have different levels of accuracy, depending on the algorithm and its training. They may also vary in accuracy for different age groups – sometimes being more accurate for older users than younger ones – or for different ethnicities or genders.

Different applications, levels of risk or legislative requirements may require services to use different levels of assurance.

Under the Part 5 duties of the UK Online Safety Act, service providers that publish pornographic content online must use **'highly effective'** age assurance methods. Ofcom's draft guidance outlines that, to be considered 'highly effective', these methods must meet criteria for technical accuracy, robustness, reliability, and fairness.[28]

The draft Irish Online Safety Code requires certain platforms to use **effective** age verification measures. These measures must ensure that children are 'not normally able to access' services devoted to adult-only video content, which includes pornography, gratuitous violence, or acts of

[‡] Spoofing is where a person or program falsely presents itself as a trusted source by recreating false data. Spoofing can occur in different ways in age assurance. For example, people may attempt to spoof facial age estimation technology by using an image or mask to appear older and trick the technology into estimating a different age.

cruelty. Age assurance measures based solely on self-declaration are not considered to be effective age verification.[29]

The ISO standard for age assurance (*ISO/IEC 27566 – Information security, cybersecurity and privacy protection – age assurance systems)* will provide a framework for understanding the different levels of assurance offered by age assurance providers. The ISO standards will be comprised of 3 parts. Part 1 (Framework) has reached a Committee Draft. A working draft of Part 2 (Technical Approaches and Guidelines for Implementation) has been submitted for approval. A working draft is being prepared of Part 3 (Benchmarks for Benchmarking Analysis). It is expected that at least Part 1 will be published in 2025.

Accuracy testing

Ofcom and the ICO commissioned research to explore how to measure the accuracy of different age assurance methods. The Age Check Certification Scheme conducted this research. It hypothesises that a headline statement of overall accuracy could be provided for each age assurance method. The report focused on measuring and comparing the accuracy of these services. However, it noted that further research is needed on bias, presentation attack vectors, fairness, and overall effectiveness.[30]

Facial age estimation testing

The United States National Institute of Standards and Technology (NIST) has opened a testing stream to update its 2014 reports on the performance of automated age estimation. This ongoing program evaluates software algorithms that analyse photos and videos of faces to estimate age. It also reports on the accuracy and computational efficiency of these algorithms. The first report from this program, published on 28 May 2024, examined six algorithms. The assessment found that most algorithms demonstrated more accurate results compared to 2014, with five of the six algorithms outperforming the most accurate algorithm from 2014. The study used four large operational datasets, as well as a dataset of images of one subject taken daily over an extended time. However, accuracy **is strongly influenced by algorithm, sex, image quality, region-of-birth, age, and interactions between these factors.** For example, some algorithms had higher error rates for people wearing glasses, and error rates were almost always higher for female faces than for male faces.[31] Results in another Australian study (against a dataset of 10,139 images) also found that accuracy varied based on ethnicity – with higher accuracy for faces categorised as Caucasian, and lower for those in the African category.[32]

One of the metrics NIST assessed in their accuracy evaluation was false positive rates for testing against a challenge age. Challenge ages are commonly used in the sale of age-restricted goods and services, such as alcohol. For example, store staff might ask for proof of age from all customers who appear to be younger than 25, instead of only those who appear to be under 18. Similarly, some age estimation technologies use a 'challenge' age to filter users. For example, a challenge age of 25 years would filter out users estimated to be over 25 and apply secondary age estimation measures to verify those assessed as between 25 and the age threshold. NIST found that false positive rates decreased with higher challenge ages.[33]

This is an ongoing program, allowing developers to re-submit algorithms to measure improvements over time. Future reports are expected to include younger datasets and consider the technology's application for online safety.

eSafety will continue to monitor independent testing reports, as well as age assurance providers' self-reported testing.

Accessibility, proportionality and flexibility

Using age assurance technology requires a proportionate and balanced approach. Different methods of implementing age assurance may feel more or less intrusive to different users. So, services should assess the specific risks on their platforms and consider complementary safety measures to determine the most appropriate and proportionate method.

When implementing age assurance, it is crucial to consider children's best interests while respecting the rights of adults to participate online. Different methods and measures will be appropriate for different online services or different parts of services.

Some methods may be more accessible or preferable for certain users and groups. For example, some age verification measures rely on identity documents. However, not all users have access to such official documents or a fixed address. Measures that require parent or carer input or consent could exclude children who don't have parents or carers to engage with these processes.

Draft guidance released by Ofcom on protecting children online considered the use of age assurance in different applications. In Ofcom's view, its use would not be proportionate for enforcing minimum ages on platforms, given limited independent evidence of some age assurance methods distinguishing between children of different age groups and that other methods, such as passport matching, may not be accessible to children. It considered this could result in a serious impact on children's ability to access these services.

Here are some considerations for industry when using age assurance technologies:

- Design measures to accurately assess the age of users inclusively and equally given their ethnicity, colour, nationality, sex, language, disability or social status.
- As children get older, the way they use technology changes. This means the risks, harms and opportunities they encounter in digital environments also change. Systems or processes to safeguard children should be capable of adapting to their evolving capacities and establishing age-appropriate measures for different age groups.[34]
- Ensure that practices for designing and implementing age assurance measures are inclusive and informed by a diverse user consultation process.
- Give users a choice over which methods to use and provide genuine, compassionate and responsive review procedures if a result is disputed. This is particularly important in the case of automated decisions. In lower-risk scenarios, consider flexible approaches beyond relying solely on hard identifiers such as government ID.[35] Self-declaration, despite being easy to bypass, may be an appropriate barrier for low-risk activities. This is especially true when it's backed up with additional safety measures.[36]

The European Commission, under the Better Internet for Children+ (BIK+) strategy, commissioned research published in April 2024 mapping types of age assurance.37 The report identified 10 requirements for the technology: proportionality; privacy; security; accuracy and effectiveness; functionality and ease of use; inclusivity and non-discrimination; furthering participation and access; transparency and accountability; notification, challenge and redressal mechanisms; and hearing the views of children.

The report found significant challenges and tensions to achieving these requirements. It also noted that some of these principles are contrasting and need to be balanced against each other. The report suggests implementing age assurance is complex, and the tool should be considered as one of many in the protection of children online.

The report also highlights how standards and clear guidance, such as the planned European standard for online age verification under the BIK+ strategy, can play a distinct role in ensuing age assurance is implemented appropriately.

Policy context and evolving environment

In the Roadmap, eSafety proposes a two-part regulatory framework to support the implementation of age assurance, if adopted.

The first part would establish the expectations and requirements for service providers within the online industry to apply age assurance and other complementary measures to prevent or limit children's access to online pornography.

In the second part, eSafety recommends a regulatory scheme be created for the accreditation and oversight of age assurance providers. This scheme would promote privacy, security, strong governance, transparency, trustworthiness, fairness, and respect for human rights.

As outlined in this paper and in the background report, several relevant government strategies across Australia, inquiries, plans, and legislative proposals are underway concerning privacy, security, human rights, and competition and consumer rights, with some focusing on biometric technologies such as facial age estimation.

There are also international developments Australia can learn from or seek to align with.

How do age assurance and complementary measures fit within eSafety's legislative and regulatory remit?

eSafety's approach to age assurance technologies is shaped by our legislative and regulatory remit as set out in the *Online Safety Act 2021* (Cth) (the Act).

Online Content Scheme

The Act regulates a wide range of online content, from the most harmful material like child sexual abuse videos or terrorism, to content that can be harmful for children, such as online pornography.

The Online Content Scheme categories this material into 'class 1' and 'class 2' based on the National Classification Scheme. The scheme empowers eSafety to issue enforceable notices that direct online service providers to take reasonable steps to remove or restrict access to this material on their platforms.

Class 2 material includes X18+ or R18+ content that may be harmful to children. This includes online pornography, high-impact depictions of violence or drug use, and from September 2024, computer games with simulated gambling, such as social casino games.

Restricted Access System

In January 2022, the eSafety Commissioner declared the Online Safety (Restricted Access Systems) Declaration 2022 ('RAS Declaration 2022'). This declaration outlines the minimum requirements that relevant online services, provided from Australia, must follow to restrict children's access to R18+ content. The current RAS Declaration does not specify or prescribe any technologies to determine age and restrict access to content.

For more information, see eSafety's website or page 357 of the Background Report.

Industry Codes and Standards

The Act provides for industry bodies or associations to develop codes to regulate class 1 and class 2 material. eSafety can register these codes if they meet certain statutory requirements including requiring that they contain appropriate community safeguards. If the codes do not meet these requirements, eSafety can instead impose mandatory standards for regulating class 1 or class 2 material provided on services within those sectors.

eSafety has taken a phased approach to developing these codes and standards. Phase 1 addresses class 1A and 1B material (categorisations set out in eSafety's initial Industry Codes Position Paper), such as child sexual exploitation and pro-terror material.

Phase 2 of the industry codes will look at measures to restrict children from accessing and being exposed to age inappropriate class 1C and class 2 material (see further information on these categories in eSafety's Industry Codes Phase 2 position paper). This work will be guided by eSafety's Roadmap, Background Report, and this issues paper. The Phase 2 Position Paper provides further guidance to industry on eSafety's expectations around codes relating to this content.

Basic Online Safety Expectations

The *Online Safety (Basic Online Safety Expectations) Determination 2022* (the Determination) sets expectations for social media, relevant electronic and designated internet service providers about keeping users safe online.

Section 12(1) of the Determination provides an expectation that service providers will take reasonable steps to prevent children's access to class 2 material. Section 12(2) provides two examples of reasonable steps: implementing age assurance mechanisms and conducting child safety risk assessments.

The Regulatory Guidance provides further examples of reasonable steps, noting the varying risks across different services. These examples apply whether a service deliberately hosts or provides access to class 2 material, permits class 2 material but is not a core aspect of the service, or prohibits class 2 material.

eSafety's Regulatory Guidance notes that age assurance mechanisms provide a degree of flexibility in how services protect children and young people from access to class 2 material. The guidance includes a wide range of examples of age assurance mechanisms and complementary measures, drawing on the findings of eSafety's Roadmap.

eSafety has the power to require reporting on services' compliance with the Basic Online Safety Expectations. Previous notices have required information on service age assurance processes, with summaries of the findings published on the eSafety website.

Independent review of the Online Safety Act

The independent review of the Act will take place in 2024. Ms Delia Rickard PSM was appointed to conduct the review and provide a report to the Minister for Communications by 31 October 2024.

eSafety's Roadmap and Background Report outlined several considerations for the review. These include the scope of content and services subject to the RAS declaration, how the ongoing government classification review intersects with online pornography under the Act, the methods eSafety can use to enforce mandatory age assurance, and how the Act applies to emerging technologies.

On 29 April 2024, the Department of Infrastructure, Transport, Regional Development, Communications, and the Arts published an issues paper and opened public consultation for the review. Submissions closed on 21 June 2024.

Domestic policy context

A number of policy issues within a domestic context involve issues relating to age assurance.

eSafety will continue to work with other Australian Government departments and agencies on policy areas related to online age assurance.

Pilot

As part of the Budget 2024-25, the Government announced $6.5 million to conduct a pilot of age assurance technology to protect children from harmful content, like pornography and other age-restricted online services. The pilot will identify available age assurance products to protect children from online harm, and test their efficacy, including in relation to privacy and security.

The trial will be overseen by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts and it will run parallel to the development of the phase 2 industry codes. eSafety will contribute to as part of a cross-government working group.

Classification

On 29 March 2023, the Australian Government released the 2020 Review of Australian Classification Regulation and announced plans to reform the National Classification Scheme.

In September 2023, the government announced that computer games with gambling-like content will be subject to new mandatory minimum classifications from September 2024. The updated *Guidelines for the Classification of Computer Games 2023* require games with in-game purchasers linked to chance (paid loot boxes) to receive a minimum M classification, and games with simulated gambling, such as social casino games, will be restricted to adults with a minimum R18+ classification.

This content now falls under the Online Content Scheme and the RAS Declaration.

A second stage of classification reform has also been announced, which seeks to address the classification frameworks, governance and regulatory arrangements.

Privacy

On 28 September 2023, the government responded to the Privacy Act Review Report. Several outcomes from the review, the government's response, and its subsequent work in this space will likely affect how age assurance technology is used in Australia, including automated decision-making and handling of biometric information.[38]

The government also supports developing a Children's Online Privacy Code, aiming to align it with international standards such as the UK Age-Appropriate Design Code. The response notes that to meet children's requirements, entities are expected to take reasonable steps to establish an individual's age with a level of certainty appropriate to the risks, such as implementing age assurance.[39]

Digital Identity

Responsibility for Australia's Digital Identity System moved from the Digital Transformation Agency to the Department of Finance in July 2023.

The Digital ID Bill 2024, together with the Digital ID (Transitional and Consequential Provisions) Bill 2024, has passed Parliament. These Bills establish the architecture and framework for a network of organisations that provide or use Digital ID services for government or commercial services. They also establish protections for citizens and their data, as well as consequences for entities that fail to comply with these protections and governance requirements.

The Act is expected to commence by November 2024.

Upon commencement, the Australian Competition and Consumer Commission (ACCC) will be the Digital ID Regulator. The Office of the Australian Information Commissioner (OAIC) will regulate the privacy aspects of Australia's Digital ID System. Within 2 years of the Act's commencement, accredited private businesses will be able to apply to join the Australian Government Digital ID System.

The NSW Government has launched several pilots of Digital ID. Digital birth certificates will become available for NSW-born citizens in 2024.[40]

As noted in the Roadmap, eSafety does not suggest requiring Australian Government digital identity to confirm age before accessing online pornography. However, age assurance technologies should be subject to accreditation and oversight standards with the same rigor and integrity as those applied to digital identity frameworks. Many digital identity service providers can also offer age assurance services, which could reduce confusion and regulatory burden.

International developments

Many jurisdictions are considering or have already implemented legislation for age assurance technology. This is not just for age-inappropriate material such as online pornography, but also for other online safety, privacy, and security issues.

Chapter 10 of eSafety's Background Report discusses various international approaches to this challenge. Momentum continues to build, and updates since the publication of the background report are outlined in Attachment D at the end of this document.

eSafety will continue its international engagement through forums such as the Global Online Safety Regulators Network, where ongoing international dialogue is critical to resolving the challenges associated with global interoperability, privacy, and technical thresholds. eSafety will observe the implementation and effectiveness of age assurance requirements, as well as monitor international pilots to bolster our knowledge, such as the upcoming EU Digital Identity Wallet to be trialled in Denmark, France, Italy, and Spain.

Jurisdictions that have passed relevant laws, such as Germany and Texas, continue to face enforcement challenges. This highlights the importance of international collaboration and coordination, which can improve compliance and reduce regulatory burden and confusion for industry and users. Regulating international or multinational organisations online is more effective with international corporation. eSafety is especially interested in what other countries are doing in these areas:

- alignment on principles such as proportionality and human rights
- relevant thresholds and criteria for age verification, and how to measure those criteria
- collaboration between regulators, especially those in online safety, privacy and competition
- how new technologies, frameworks and infrastructure can support using age assurance in ways that preserve privacy – such as developments relating to decentralised digital identity or double-blind exchanges

- enforcement challenges, including challenges to legal jurisdiction and circumvention of enforcement actions
- ways to support complementary measures across the digital ecosystem.

Conclusion

Age assurance can be an important element in online safety, especially for children, but it must be part of a broader set of complementary safety measures to protect the rights of users.

Upcoming initiatives include the second phase of Industry Codes, an age assurance pilot, and the outcomes from the Privacy Act review, including obligations for children's privacy, and the development of Digital ID frameworks. These changes, along with international developments, will likely set new obligations for online services and influence how age assurance is used Australia.

Attachment A - Reading guide to eSafety's Background Report

Each chapter includes a **KEY POINTS** section for readers who want a quick overview. We recommend reading the entire report to understand the broad range of technical and social issues. However, we also offer additional guides to this document tailored to different needs.

For a **QUICK OVERVIEW**, read:

- Section: Scope (page 10)
- Key Points of Chapter 5 (page 47)
- Key Points of Chapter 8 (page 136)
- eSafety next steps and recommendations for the Australian Government (page 303 and 374)

For **INDUSTRY**, read:

- Section: When, where and why are children encountering pornography? (Chapter 5, page 54)
- Chapter 6 - The digital ecosystem (page 93)
- Chapter 8 - Age Assurance technology interventions (page 16)
- Chapter 11 - Other technological interventions (page 257)
- Chapter 12 - Opportunities for change (page 283)
- **Don't miss**: Summary table of considerations for Industry (page 302)

For **POLICY-MAKERS**, read:

- Chapter 4 - A human rights-based approach (page 33)
- Chapter 9 - The enabling environment for age assurance technologies (page 198)
- Chapter 10 - International developments on age assurance (page 231)
- Chapter 12 - Opportunities for change (page 283)
- Chapter 14 – The online safety act: eSafety's current functions and future opportunities to prevent and minimise harms to children from online pornography (page 346)

For **RESEARCHERS**, read:

- Chapter 3 - Methodology (page 16)
- Chapter 5 - Evidence of harm and impacts of online pornography on children (page 47)
- Chapter 7 - the future of online pornography (page 112)

For **EDUCATORS**, read:

- Section: When, where and why are children encountering pornography? (Chapter 5, page 54)
- Chapter 13 - the role of education in protecting and empowering children (page 310)

Attachment B – Examples of complementary safety measures

Measure	Overview
Filters (service and device level)	Block access to content that may be illegal, harmful, or not age appropriate.
Parental controls	Software tools that allow you to monitor and limit what your child sees and does online. They can also be built into products which allow parents to control child accounts: • Use of parental controls should be informed by the evolving capacities of a child (such as age, digital literacy skills and maturity). As children get older, a graduated approach to use and easing controls is often needed. • Most parental controls and filters need to be installed and configured by parents. This presents challenges, as children that are vulnerable online are generally more vulnerable offline. • There are several potential barriers to uptake, including cost, awareness, accessibility and digital literacy.
User controls, safety and privacy settings	• Place limits on the types of activities a user can engage in, who they can connect with, and what user information is shared with others. • Sensitive content warnings which blur incoming messages or content, first asking users if they want to see the content. • Tools which support users to exercise greater control over content they see.
Content moderation and curation	Systematic practice of vetting content posted online to determine its appropriateness. This can include: • Algorithmic detection identifying or blocking inappropriate content • Human moderators reviewing and classifying problematic content • Community moderators reporting content/taking enforcement action • Users reporting inappropriate content or underage users.
Policies and procedures	Policies should outline any age restrictions, whether age-restricted goods or services are provided and relevant expectations and responsibilities of the organisation and consumers. Procedures should transparently outline how organisations manage access to age restricted goods and services, how they prevent underage access and how underage access can be reported. Policies and procedures should be: • Easily accessible in trust and safety or policy centres, or where they can provide the most friction to underage access (e.g. sign up pages).

Measure	Overview
	• Explain how age assurance measures are implemented and how personal data is managed and protected. • Reported on in transparency reports to demonstrate effectiveness.
Educational resources	• Resources on how age assurance technologies work and how to be discerning over where personal data is shared are important for creating informed consumers. • Links to educational resources can be shared with users when age-restricted content is searched for, or is being uploaded. • Resources should cover online risks and what to do if users encounter something harmful. Resources should be tailored to different audiences- such as, children, young people, parents, carers, educators.

Attachment C – Factors considered by eSafety in the Roadmap

Design factors considered include:

- level of assurance
- feasibility, including whether the technology is ready to be rolled out and effective in practice
- extent and sensitivity of the data required for the technology to operate
- security and technical integrity of the technology
- accessibility, barriers to inclusion and potential for bias

Implementation factors considered at the product or provider level and/or the enabling environment level include:

- transparency and accountability in relation to decision-making, and availability and accessibility of appeals processes
- governance and risk management processes
- flexibility to account for different business models
- certification, accreditation or auditing against minimum standards
- compliance with privacy legislation
- trustworthiness of the technology (both perceived and actual)
- independent oversight
- availability of multiple options to enable customer choice
- fairness, accessibility and equity
- compatibility with human rights
- proportionality to the risks of harm based on the available evidence.

Attachment D – Updates to International efforts

Regulatory Developments

Country / Region	Developments since the Roadmap
Europe EU Audiovisual Media Services Directive (AVMSD) Digital Services Act (DSA)	<u>Digital Services Act</u> Since 17 February 2024, with the exception of small and microenterprises, all online platforms and search engines must comply with the general obligations under the DSA. If a service reaches more than 10% of the EU population (about 45 million), the service is designated as a 'very large online platform' (VLOP) and has **extra obligations** under the DSA.[41] Within four months of being designated as a VLOP, these services must adopt additional measures: • more diligent content moderation • stronger protection of minors – (VLOPs must design their services to address and prevent risks to the wellbeing of children, **which may include age verification tools**) • be more transparent and accountable, including providing access to their advertising repository to ensure oversight of targeted advertising In December 2023, three pornography services (Pornhub, Stripchat and Xvideos) were designated as VLOPs. They join 17 other services previously designated as a VLOP and two 'very large online search engines'.[42] However, in March 2024, Pornhub, through its parent company Aylo, filed a legal challenge against the European Union. They are disputing Pornhub's designation as a VLOP and the user count that qualifies Pornhub as a VLOP. Pornhub is also opposing the mandate to make its advertising repository public and is seeking a court ruling to suspend its advertising-related obligations under the DSA.[43] On 16 May 2024, the Commission opened formal proceedings against Meta for possible breaches of the DSA. The Commission is assessing if Meta's age verification tools to prevent minors from accessing inappropriate content are reasonable, proportionate, and effective. The Commission may take further action if it finds Meta has infringed the DSA.[44] <u>Digital Services Co-ordinators</u> The Commission and Digital Services Co-ordinators (DSCs) supervise and enforce the obligations under the DSA. Each member state was required to appoint a DSC by 17 February 2024.

Country / Region	Developments since the Roadmap
	DSCs enforce the DSA in their countries, with the authority to access to data, order inspections, impose infringement fines on providers, and certify trusted flaggers to detect and remove illegal content. As of 15 April 2024, 19 member states have appointed a DSC.[45] Some of the remaining eight, such as France, have entered into interim agreements with the Commission pending their official DSC appointment.[46] However, on 24 April 2024, the European Commission commenced infringement procedures against Estonia, Poland and Slovakia for failing to designate their DSCs and Cyprus, Czechia and Portugal for failing to sufficiently empower their DSCs.[47] These states have two months to comply. Better Internet for Kids (BIK+) strategy In 2022, the European Commission adopted a new strategy for children's safety online – the Better Internet for Kids (BIK+) strategy.[48] This strategy aims to: • develop a comprehensive **EU code of conduct for age-appropriate design, covering topics including age assurance**, data protection, and clear and accessible information • support an EU-wide digital proof-of-age system A special group of academics, industry experts and civil society members was set up to develop this code. It convened for the first time on 13 July 2023, with the aim to publish a code by mid-2024.[49] In May 2024, BIK+ published a self-assessment tool and questionnaire to help digital service providers evaluate their platforms' impact on child safety online. The tool aids service providers in determining the need for age assurance, assessing the required level of age assurance, and developing a balanced age assurance process. The tool serves as guidance rather than a legal compliance mechanism. Digital Identity Regulation On 26 March 2024, the European Union adopted the Digital Identity Regulation, introducing the EU Digital Identity Wallet. By 2026, all members states must make a Digital Identity Wallet available to its citizens and recognise Digital Identity Wallets from other states. The Digital Identity Wallet will allow for the authentication of identities and share information such as age without disclosing other personal details.[50] The Digital Identity Wallet will be optional for citizens, not mandatory. Starting April 2023, four large scale pilots involving 360 public and private entities across 26 member states began testing a range of everyday use cases for the Digital Identity Wallet. They are expected to be completed by 2025.[51]
United Kingdom Online Safety Act	Online Safety Act The Online Safety Bill became law on 26 October 2023. Under the Online Safety Act, services which publish or display pornography must have **highly effective age assurance measures** so that children cannot normally access primary priority content (PPC) on their services. PPC includes

Country / Region	Developments since the Roadmap
	pornography and content which promotes suicide, self-harm or eating disorders. This extends to services based in the UK or targeting the UK market. Services with pornographic content include online services that publish or display certain pornographic content in the form of videos, images or audio. They also include services which allow users to upload and share pornographic content which can be viewed by other users of the services. These services could be user-to-user sites and apps or video-sharing platforms. Ofcom Draft Guidance Ofcom published draft guidance for phase two of their online safety regulation plan focusing on child safety and pornography, which includes a non-exhaustive list of age assurance methods Ofcom currently considers to be 'highly effective'.[52] The draft guidance closed for consultation on 5 March 2024. On 18 January 2024, the UK Information Commissioner's Office published an **updated opinion on age assurance**. The updated opinion provides further advice to industry to inform their approach to age assurance, including reflecting technological developments and meeting data protection obligations.[53] On 25 March 2024, Ofcom also launched phase three of their online safety regulation plan focusing on transparency, user empowerment and other duties on categorised services with a call for evidence to inform additional duties for categorised services, including user identity verification duties. The call closed on 20 May 2024.[54] Ofcom anticipate they will publish guidance on transparency reporting in Spring 2024 and publish final codes of practice and guidance by late 2025, with Parliamentary approval expected in Spring 2026. On 8 May 2024, Ofcom released draft regulatory guidance on the protection of children for public feedback. Its guidance includes the draft Children's Safety Codes, which recommends measures online services should take to protect children from online harms as part of their duties under the Act. The codes propose that online services adhere to the following obligations: • Assess whether children are likely to access their service or part of their service. • Conduct a children's risk assessment to identify risks that their service pose to children. Services with highly effective age assurance which can confirm that children are not likely to access their service or part of their service may be exempt. • Implement safety measures to mitigate the risks to children. The codes propose more than 40 safety measures, such as robust age checks and algorithms which filter out harmful content from children's feeds. • Keep risks and safety measures under review.[55] The consultation will close on 17 July. Ofcom intends to publish the final Children's Safety Codes of Practice by Spring 2025. Services will then have three months to conduct children's risks assessments.

Country / Region	Developments since the Roadmap
United States	Age verification for access to online pornography Several states have introduced **state-based restrictions requiring age verification for online pornography**. These include Louisiana, Mississippi, Virginia, Utah, Arkansas, North Carolina, Texas and Montana. Each state has its own definition of what constitutes 'age verification'.[56] Accordingly, the detail of these restrictions varies state by state. For example, Utah and Virginia allow various verification methods, Mississippi requires a drivers' licence, and Louisiana permits the use of LAWallet, the state's digital driver's license, through third party identification sites. The effectiveness of these measures is unclear. Some platforms appear to be complying, while others continue to offer unrestricted access or have blocked users from particular states rather than apply age assurance measures.[57] Media reports suggest an increase in VPN use or interest in states where services have blocked users.[58] The Free Speech Coalition and operators of pornographic sites including Pornhub and xnxx.com sued Texas over its age verification law, alleging it infringes on free speech. On 9 March 2024, the 5th US Circuit Court of Appeals (CCA) upheld the legislation, finding the plaintiffs were unlikely to succeed in their constitutional challenge.[59] The plaintiffs sought to stay the CCA decision in the Supreme Court. However, on 2 May 2024, their request was denied.[60] Age verification for social media usage Some states are also seeking to legislate age verification to restrict minors' access to social media. States such as Utah, Texas and Arkansas want to restrict social media to users over 18, unless they have parental consent.[61] Meanwhile, Florida aims to ban social media accounts for those under 14 and require parental consent for 15–16-year-olds.[62] These proposed laws face legal challenges for potentially violating constitutional rights to freedom of speech and freedom of expression. Critics also have concerns about restricted access to information on reproductive healthcare, gender and sexuality, especially for marginalised groups.[63] Recent lawsuits by Netchoice against Ohio[64] and Arkansas,[65] and by the Foundation for Individual Rights and Expression's against Utah, highlight these concerns.[66]
Canada	Canada has drafted bills regulating online harms and children's exposure to inappropriate content online. On 13 December 2023, Canada's Senate passed the *Protecting Young Persons from Exposure to Pornography Act* (Bill S-210). If this bill becomes law, it will be illegal for any organisation to make available sexually explicit material on the Internet to anyone under 18.[67] The Governor in Council may set regulations prescribing age-verification methods. Before prescribing an age-verification method, the method should be considered against the following criteria: that the method is reliable, maintains user privacy and protects personal information, collects and uses personal information only to verify age, destroys any personal information collected after verification, and follows best practices in age verification and privacy protection.[68]

Country / Region	Developments since the Roadmap
	On 26 February 2024, Canada also introduced the *Online Harms Act* through Bill C-63. This bill is currently at its second reading in the House of Commons.[69] If it passes, online platforms will have to monitor for and remove harmful content, such as child sexual exploitation material and content that incites violent extremism. Online platforms will also be subject to a **duty to protect children, including by integrating age-appropriate design features**.[70] This might mean services have to use age assurance measures if children are accessing their services.
France	Under Article 23 of Act No. 2020-936 of 30 July 2020 to Protect Victims of Domestic Violence, online publishers must prevent those under the age of 18 from accessing online pornography.[71] This law applies to all online adult content providers whose services are available in France. Under the legislation, non-compliant services could be blocked. In December 2021, the French Audiovisual and Digital Communication Regulatory Authority (Arcom) issued enforcement notices to five pornographic websites, including Pornhub, XHamster, and Xvideos, requiring them to prove they were preventing access to minors in line with their legislative requirements.[72] In September 2022, MindGeek (as Aylo was then known) raised a constitutional challenge against the legislation's requirements.[73] This case is still pending review. On 7 July 2023, France passed legislation (Law No. 2023-566, colloquially known as the 'Digital Majority Law') requiring parental consent for minors under the age of 15 years to hold social media accounts. Social media services are required to verify the age of new registrants and verify parental consent for new registrants under the age of 15 years, failing which services must decline registrants under 15 years. Services have one year from the date of effect to comply with their legal obligations for new subscribers and two years to apply the requirements to existing users.[74] On 10 April 2024,[75] France adopted a new bill (SREN – Secure and Regulate Digital Space). SREN authorises Arcom to request for the blocking or delisting of online public communication services and video-sharing platform services that disseminate pornographic content which allow their services to remain accessible to minors. Arcom is also empowered to issue financial sanctions for non-compliance. The European Commission considered that the scope of SREN, particularly its age verification requirements, would fall within the DSA.[76] SREN also requires Arcom to publish a technical reference guide outlining the requirements for age verification systems on pornographic sites. Arcom published their draft standards regarding the minimum technical requirements for age verification systems for access to online pornographic content on 11 April 2024. The draft minimum technical requirements propose several criteria for age verification, including the following: • Services must provide their best efforts to limit possible circumvention of the age verification solutions they use. The age verification solution must be robust and must not allow sharing of proof of age. • Age verification must take place at every visit to a service. The use of reusable proofs of age (such as through a digital wallet) is permitted. • Age verification solutions must be compliant with the GDPR including the principles of data minimisation and privacy.

Country / Region	Developments since the Roadmap
	The standards were open for public consultation until 13 May 2024.[77]
Spain	The Royal Spanish Mint and the National Data Protection Agency (AEPD) are developing technology that enables users to verify and share their age, aimed at preventing minors from accessing to online pornography. Initial reports suggest this technology uses government identification for age verification and shares the verified age with websites via an app, QR code or certificate.[78] Spain hope to launch the age verification pilot project by mid-2024.[79] In December 2023, the AEPD published practical guidance on age verification, focused on aiming to protect minors from inappropriate content online.[80] The guidance stresses that age verification systems must follow the principles of data minimisation, privacy by design and default and accountability. It emphasises the importance of anonymity and says providers should not process personal data when verifying a user's age. The guidance also recommends consulting parents and guardians when deciding which types of content are inappropriate for minors. On 16 January 2024, the Spanish Government approved a three-pronged approach. In addition to an age verification system, it intends to establish working groups, and draft laws to prevent minors from accessing online adult content. On 15 March 2024, the AEPD began working with the European Data Protection Board to develop guidelines for age verification. The AEPD criticised current age verification systems as inefficient for protecting children, lacking assurance, or containing risks such as exposing the location of minors, mass profiling and collecting unnecessary data. A Working Group, chaired by the Ministry for Digital Transformation, was created to improve protection for minors when accessing online content, while respecting privacy and data protection.[81]
Germany	In several proceedings, state media authorities and the KJM have issued blocking orders to access providers for the first time about pornographic content from foreign providers. The content could be accessed without restrictive barriers, as is required by the *State Treaty on the Protection of Minors in the Media*. The providers filed a lawsuit against the decisions arguing that the *Sta Treaty* was not applicable to them. However, it was determined that an exception to the country-of-origin principle is possible if pornography i offered without technical age restrictions.[82]
Ireland Broadcasting Act 2009 as amended by the Online Safety and Media Regulation Act 2022 **Draft Online Safety Code**	Coimisiún na Meán (CnaM), Ireland's online safety regulator, is currently developing Ireland's first Online Safety Code. CnaM published its Draft Online Safety Code (draft code) and related matters for Video-Sharing Platform Services (VSPSs) for consultation between 8 December 2023 to 19 January 2024.[83] Once finalised, the code will set out obligations for VSPS in how they address illegal content, age-appropriate content, online hate, terrorism, extremism, violence and discrimination. On 9 January 2024, CnaM designated Facebook, Instagram, YouTube, Udemy, TikTok, LinkedIn, X, Pinterest, Tumblr and Reddit as VSPSs.[84]

Country / Region	Developments since the Roadmap
	The draft code requires VSPSs to use effective age verification measures. For example, VSPSs which permit pornography or depictions of gross or gratuitous violence must use effective age assurance so minors cannot normally see such content. The Commission does not regard measures based solely on self-declaration as an effective form of age verification. However, it may be adequate for preventing under-age users from low-risk services when combined with usage-based estimation.[85] CnaM has reported it is working with the Commission on a pan-European approach to age assurance, with the aim of achieving similar protections for children on platforms across Europe.[86] In response to its public consultation, on 27 May 2024 CnaM published an updated draft code, which it submitted to the European Commission.[87] Once the Technical Regulations Information System Directive process concludes, which includes a 3–4-month standstill period, CnaM will finalise and apply the code to the designated VSPS in Ireland. It is expected the code will be finalised later this year.

[1] United Nations, *General Comment No. 25 on children's rights in relation to the digital environment*, 2 March 2021, paragraph 19 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[2] Ofcom, *A third of children have false social media age of 18+*, 5 January 2024, https://www.ofcom.org.uk/news-centre/2022/a-third-of-children-have-false-social-media-age-of-18

[3] P Diwanji, Meta, *How do we know someone is old enough to use our apps?*, 27 July 2021, https://about.fb.com/news/2021/07/age-verification/

[4] eSafety Commissioner, *Public perceptions of age verification for limiting access to pornography*, 15 October 2021, https://www.esafety.gov.au/research/public-perceptions-age-verification-for-limiting-access-pornography

[5] Google, *Access age-restricted content & features*, n.d., https://support.google.com/accounts/answer/10071085

[6] eSafety Commissioner, *Basic Online Safety Expectations: Summary of industry responses to mandatory transparency* notices, October 2023, page 82 https://www.esafety.gov.au/industry/basic-online-safety-expectations

[7] Yubo, *Yubo's new age verification feature helps keep you safe*, 2022, https://www.yubo.live/blog/yubos-new-age-verification-feature-helps-keep-you-safe

[8] Meta, *Why Instagram is asking for your birthday*, n.d., https://help.instagram.com/366075557613433

[9] TikTok, *Underage appeals on TikTok*, n.d., https://support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok#1

[10] Tinder, *Tinder announces ID Verification pilot in Australia and New Zealand*, 6 October 2023, https://au.tinderpressroom.com/news?item=122572

[11] Roblox, *Age ID Verification*, n.d., https://en.help.roblox.com/hc/en-us/articles/4407282410644-Age-ID-Verification

[12] eSafety Commissioner, *Basic Online Safety Expectations: Summary of industry responses to the first mandatory transparency notices*, December 2022, page 56 https://www.esafety.gov.au/industry/basic-online-safety-expectations

[13] eSafety Commissioner, *Basic Online Safety Expectations: Summary of industry responses to mandatory transparency* notices, October 2023, page 145 https://www.esafety.gov.au/industry/basic-online-safety-expectations

[14] NSW Liquor & Gaming, *Checking evidence of age*, n.d., https://www.liquorandgaming.nsw.gov.au/working-in-the-industry/serving-alcohol-responsibly/managing-under-18s/checking-evidence-of-age

[15] Department of Social Services, *Gambling reforms*, 15 December 2023, https://www.dss.gov.au/communities-and-vulnerable-people-programs-services-gambling/gambling-reforms

[16] Sportsbet, *How do I verify my account online?*, n.d., https://helpcentre.sportsbet.com.au/hc/en-us/articles/115006475128-How-Do-I-Verify-My-Account-Online

[17] E Finkle, Meta, *Bringing Age Verification to Facebook Dating*, 5 December 2022, https://about.fb.com/news/2022/12/facebook-dating-age-verification/

[18] PlayStation, *Age verification frequently asked questions*, n.d., https://www.playstation.com/en-gb/support/account/age-verification-faq/

[19] Yoti, *How OnlyFans became the first UK subscription-based platform to protect children and create age-appropriate experiences*, 16 June 2023, https://www.yoti.com/blog/how-onlyfans-became-the-first-uk-subscription-based-platform-to-protect-children-and-create-age-appropriate-experiences/

[20] Ofcom, *Investigating OnlyFans' compliance with its duties to protect under-18s from restricted material and respond to information requests*, 1 May 2024, https://www.ofcom.org.uk/online-safety/protecting-children/cw_01283/

[21] eSafety Commissioner, *Restricted access system*, 25 March 2022, https://www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system

[22] Ofcom, *Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services*, 5 December 2023, page 15, https://www.ofcom.org.uk/online-safety/protecting-children/guidance-service-providers-pornographic-content/

[23] Australian Competition and Consumer Commission, *Digital Platform Services Inquiry – Interim Report 7: Report on expanding ecosystems of digital platform service providers*, September 2023, p.g 94 https://www.accc.gov.au/about-us/publications/serial-publications/digital-platform-services-inquiry-2020-25-reports/digital-platform-services-inquiry-september-2023-interim-report

[24] Information Commissioner's Office, *Age assurance for the Children's code*, 15 January 2024 https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/

[25] Laboratoire d'Innovation Numérique de la CNIL, *[Follow-up] – Age verification: the economic argument*, 19 July 2023, https://linc.cnil.fr/follow-age-verification-economic-argument

[26] E Pinedo, Reuters, *Spain readies age-checking tech to protect children from adult online content*, 15 December 2023, https://www.reuters.com/world/europe/spain-readies-age-checking-tech-protect-children-adult-online-content-2023-12-14/

[27] euCONSENT, *euCONSENT announces the AgeAware App – device-based online age assurance*, 12 April 2024, https://euconsent.eu/euconsent-announces-the-ageaware-app-device-based-online-age-assurance/

[28] Ofcom, *Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services*, 5 December 2023, page 17, hhttps://www.ofcom.org.uk/online-safety/protecting-children/guidance-service-providers-pornographic-content/

[29] Coimisiún na Meán, *Draft Online Safety Code*, 27 May 2024, page 10 https://www.cnam.ie/publications/

[30] T Allen, L McColl, K Walters and M Lyon, *Measurement of Age Assurance Technologies Part 2 – Current and short-term capability of a range of age assurance measures*, 2023
hhttps://www.drcf.org.uk/publications/papers/measurement-of-age-assurance-technologies

[31] K Hanaoka, M Ngan, J Yang, G W Quinn, A Hom and P Grother, National Institute of Standards and Technology, *Face Analysis Technology Evaluation: Age estimation & verification*, 28 May 2024,
https://pages.nist.gov/frvt/html/frvt_age_estimation.html

[32] Z Stardust, A Obeid, A McKee and D Angus, *Mandatory age verification for pornography access: Why it can't and won't 'save the children'*, 11 June 2024, https://journals.sagepub.com/doi/10.1177/20539517241252129

[33] K Hanaoka, M Ngan, J Yang, G W Quinn, A Hom and P Grother, National Institute of Standards and Technology, *Face Analysis Technology Evaluation: Age estimation & verification*, 28 May 2024,
https://pages.nist.gov/frvt/html/frvt_age_estimation.html

[34] United Nations, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, 2 March 2021, paragraph 12 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[35] For example, AUSTRAC have released guidance about flexible approaches for customer identification: AUSTRAC, *Assisting customers who don't have standard forms of identification*, 17 January 2024,
https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/assisting-customers-who-dont-have-standard-forms-identification

[36] Ofcom's current draft guidance notes that self-declaration is insufficient to prevent children's access to online pornography. Ofcom, *Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services*, 5 December 2023, page 16,
https://www.ofcom.org.uk/online-safety/protecting-children/guidance-service-providers-pornographic-content/

[37] M Raiz Shaffique and S van der Hof, European Commission Directorate-General for Communications Networks, *Research report: Mapping age assurance typologies and requirements*, February 2024,
https://op.europa.eu/en/publication-detail/-/publication/215f6c72-fe04-11ee-a251-01aa75ed71a1/language-en

[38] Australian Government, *Government response: Privacy Act review report*, 2023, page 28, proposal 13.2
https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report

[39] Australian Government, *Government response: Privacy Act review report*, 2023, page 14,
https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report

[40] NSW Government, *Customer Service – projects and initiatives: Digital birth certificate*, n.d.
https://www.nsw.gov.au/departments-and-agencies/customer-service/projects-and-initiatives

[41] European Commission, *Commission designates second set of Very Large Online Platforms under the Digital Services Act*, 20 December 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6763

[42] European Commission, *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*, 25 April 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413

[43] The Economic Times, *Why has Pornhub sued the European Union?*, 8 March 2024,
https://economictimes.indiatimes.com/news/international/world-news/why-has-pornhub-sued-the-european-union/articleshow/108319555.cms?from=mdr

[44] European Commission, *Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram*, 16 May 2024,
https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664

[45] European Commission, *Digital Services Coordinators*, 28 May 2024, https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs

[46] Euronews, *Platform rules to apply this month as member states lag on oversight personnel*, 7 February 2024, https://www.euronews.com/next/2024/02/07/platform-rules-to-apply-this-month-as-member-states-lag-on-oversight-personnel

[47] European Commission, *April infringement package: key decisions*, 24 April 2024,
https://ec.europa.eu/commission/presscorner/detail/en/inf_24_1941

[48] European Commission, *New EU strategy to protect and empower children in the online world*, 11 May 2022,
https://digital-strategy.ec.europa.eu/en/news/new-eu-strategy-protect-and-empower-children-online-world

[49] European Commission, *Frequently asked questions – Special group on the EU code on age-appropriate design*, 15 December 2022, https://digital-strategy.ec.europa.eu/en/miscellaneous/frequently-asked-questions-special-group-eu-code-age-appropriate-design

[50] The European Digital Identity Regulation, *The European eID*, n.d. https://www.european-digital-identity-regulation.com/

[51] European Commission, *What are the Large Scale Pilots Projects*, n.d. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects

[52] Ofcom, *Guidance on age assurance and other Part 5 duties for service providers publishing pornographic content on online services Annex 2*, 5 December 2023, https://www.ofcom.org.uk/online-safety/protecting-children/guidance-service-providers-pornographic-content/

[53] Information Commissioner's Office, *ICO publishes updated Commissioner's Opinion on age assurance for the Children's code*, 18 January 2024, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/01/ico-publishes-updated-commissioner-s-opinion-on-age-assurance-for-the-children-s-code/

[54] Ofcom, *Call for evidence: Third phase of online safety regulation*, 25 March 2024, https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/third-phase-of-online-safety-regulation/

[55] Ofcom, *Consultation: Protecting children from harms online*, 8 May 2024 https://www.ofcom.org.uk/consultations-and-statements/category-1/protecting-children-from-harms-online

[56] S Forland, N Meysenburg and E Solis, Open Technology Institute, *Age verification: The complicated effort to protect youth online*, 22 April 2024, page 14, https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/executive-summary/

[57] S E Jenkins, CBS News, *Pornhub block access in Texas in dispute over age verification law*, 14 March 2024, https://www.cbsnews.com/texas/news/leading-adult-entertainment-website-blocks-service-in-texas/

[58] C Lima-Strong and D DiMolfetta, The Washington Post, *Utah's porn crackdown has a VPN problem*, 5 May 2023, https://www.washingtonpost.com/politics/2023/05/05/utahs-porn-crackdown-has-vpn-problem/

[59] B Pierson, Reuters, *US court upholds Texas law mandating age verification for online porn*, 9 March 2024, https://www.reuters.com/legal/us-court-upholds-texas-law-mandating-age-verification-online-porn-2024-03-08/?ref=platformer.news

[60] A Chung, Reuters, *US Supreme Court will not halt Texas age verification for online porn*, 1 May 2024, https://www.reuters.com/world/us/us-supreme-court-wont-halt-texas-age-verification-online-porn-2024-04-30/

[61] Utah State Legislature, *Social Media Regulation Amendments*, 2024; https://le.utah.gov/~2024/bills/static/SB0194.html, State of Texas, *Securing Children Online through Parental Empowerment Act*, 2023, https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB00018F.pdf#navpanes=0; Arkansas State Legislature, *Social Media Safety Act*, 2023, https://www.arkleg.state.ar.us/Bills/Detail?id=SB396&ddBienniumSession=2023%2F2023R

[62] Governor Ron DeSantis, *Governor DeSantis signs legislation to protect children and uphold parental rights*, 25 March 2024, https://www.flgov.com/2024/03/25/governor-desantis-signs-legislation-to-protect-children-and-uphold-parental-rights/

[63] M Kelly, The Verge, *Child safety bills are reshaping the internet for everyone*, 30 August 2023, https://www.theverge.com/2023/8/29/23849375/kosa-child-safety-free-speech-louisiana-utah-parental-consent

[64] Spectrum News, *A judge has temporarily halted enforcement of an Ohio law limiting kids' use of social media*, 9 January 2024, https://spectrumnews1.com/oh/columbus/news/2024/01/09/social-media-law-blocked

[65] ACLU, *Judge blocks Arkansas law that would have placed unconstitutional age-verification and parental consent requirements on social media users*, 1 September 2023, https://www.aclu.org/press-releases/judge-blocks-arkansas-law-that-would-have-placed-unconstitutional-age-verification-and-parental-consent-requirements-on-social-media-users

[66] FIRE, *Lawsuit: Utah's clumsy attempt to childproof social media is an unconstitutional mess*, 16 January 2024, https://www.thefire.org/news/lawsuit-utahs-clumsy-attempt-childproof-social-media-unconstitutional-mess

[67] Parliament of Canada, *Bill S-210*, 18 April 2023, section 5, https://www.parl.ca/DocumentViewer/en/44-1/bill/S-210/third-reading

[68] Parliament of Canada, *Bill S-210*, 18 April 2023, section 11, https://www.parl.ca/DocumentViewer/en/44-1/bill/S-210/third-reading

[69] Parliament of Canada, *Bill C-63*, 26 February 2024, https://www.parl.ca/LegisInfo/en/bill/44-1/C-63

[70] Parliament of Canada, *Bill C-63*, 26 February 2024, sections 64 and 65, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-63/first-reading

[71] Légifrance, *Authenticated Electronic Official Journal No. 0187* (Translated), 2020, https://www.legifrance.gouv.fr/download/pdf?id=shLVial2GFAvXVHYawAie63PzXyh2U2x_naRfEud_Wg=

[72] Reuters, *French court to rule on plan to block porn sites over access for minors*, 7 September 2022 https://www.reuters.com/world/europe/french-court-rule-plan-block-porn-sites-over-access-minors-2022-09-06/

[73] J Apostle and M Hennessey, Orrick, *Online content in France: Challenge raised to block online porn websites*, 12 September 2022 https://www.orrick.com/en/Insights/2022/09/Online-Content-in-France-Challenge-Raised-to-Block-Online-Porn-Websites

[74] Légifrance, *Draft law to secure and regulate the digital space* (ECOI2309270L) (Translated), 20 October 2023, https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047533100/

[75] France 24, *What's in the bill to secure the Internet, definitively adopted by the Assembly* (Translated), 10 April 2024, https://www.france24.com/fr/france/20240410-le-projet-de-loi-pour-s%C3%A9curiser-internet-d%C3%A9finitivement-adopt%C3%A9-apr%C3%A8s-un-ultime-vote-%C3%A0-l-assembl%C3%A9e

[76] BCLP Law, *The French law on the regulation of games including NFT is passed: Place your bets*, 22 April 2024, https://www.bclplaw.com/en-US/events-insights-news/the-french-law-on-the-regulation-of-games-including-nft-is-promulgated-place-your-bets.html

[77] Arcom, Public consultation on the draft standard setting out the minimum technical requirements for age verification systems for access to pornographic content online (Translated), 11 April 2024, https://www.arcom.fr/vos-services-par-media/consultations-publiques/consultation-publique-sur-le-projet-de-referentiel-determinant-les-exigences-techniques-minimales-applicables-aux-systemes-de-verification-de-lage-mis-en-place-pour-acces-contenus-pornographiques-en-ligne

[78] E Pinedo, *Spain readies age-checking tech to protect children from adult online content*, 15 December 2023, https://www.reuters.com/world/europe/spain-readies-age-checking-tech-protect-children-adult-online-content-2023-12-14/

[79] Euronews, *Spanish government to regulate online porn access to protect minors*, 16 January 2024, https://www.euronews.com/2024/01/16/spanish-government-to-regulate-online-porn-access-to-protect-minors

[80] Agencia Española Protección Datos, *Decalogue of principles: Age verification and protection of minors from inappropriate content,* December 2023, https://www.aepd.es/guides/decalogue-principles-age-verification-minors-protection.pdf

[81] Agencia Española Protección Datos, Agency encourages development of European panel guidelines for age verification systems on internet, 15 March 2024, https://www.aepd.es/en/press-and-communication/press-releases/agency-encourages-development-of-european-panel-guidelines-for-age-verification-systems-on-internet

[82] Kommission für Jugendmedienschutz, *10. Tätigkeitsbericht* (10th Activity Report by the German Commission for Youth Media Protection), 12 May 2023, https://www.kjm-online.de/publikationen/taetigkeitsberichte

[83] Coimisiún na Meán, *Consultation document: Online safety*, 8 December 2023, https://www.cnam.ie/coimisiun-na-mean-opens-public-consultation-on-irelands-first-online-safety-code/

[84] Coimisiún na Meán, *Coimisiún na Meán designates Video-Sharing Platform Services*, 9 January 2024, https://www.cnam.ie/coimisiun-na-mean-designates-video-sharing-platform-services/

[85] Coimisiún na Meán, *Consultation document: Online safety*, 8 December 2023, page 17, https://www.cnam.ie/coimisiun-na-mean-opens-public-consultation-on-irelands-first-online-safety-code/

[86] Coimisiún na Meán, *Revised Online Safety Code Q&A – 27 May 2024*, 27 May 2024, page 4, https://www.cnam.ie/coimisiun-na-mean-to-notify-online-safety-code-to-european-commission/

[87] Coimisiún na Meán, *Coimisiún na Meán to notify Online Safety Code to European Commission*, 27 May 2024, https://www.cnam.ie/coimisiun-na-mean-to-notify-online-safety-code-to-european-commission/